UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/913,453	08/14/2001	Graeme John Proudler	B-4276PCT 619003-1	9595

22879 7590 08/29/2006

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
PHAN, TRI H	

ART UNIT	PAPER NUMBER
2616	

DATE MAILED: 08/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

A

Office Action Summary	Application No.	Applicant(s)	
	09/913,453	PROUDLER ET AL.	
	Examiner	Art Unit	
	Tri H. Phan	2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 June 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)□ Claim(s) *1-5,7,8,12-25 and 27-30* is/are rejected.

7)□ Claim(s) *6,9-11 and 26* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: _____.

DETAILED ACTION

Response to Amendment/Arguments

1. This Office Action is in response to the Appeal Brief filed on June 16th, 2006. In view of the following new grounds of rejection, the previous final Office action has been withdrawn. Claims 1-30 are now pending in the application.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 16 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 16, line 6, the phrase "as the case may be" is vague and indefinite because it is unclear whether the limitation(s) belonging is part of the claimed invention or not, and the resulting claim does not clearly set forth the metes and bounds of the patent protection desired.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

> invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-5, 7-8, 12-25, and 27-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Boebert et al.** (U.S.5,822,435; hereinafter refer as '**Boebert**') in view of **Beckman et al.** (U.S.6,385,724; hereinafter refer as '**Beckman**').

- In regard to claims 1 and 21, **Boebert** discloses, *the computing apparatus* ('workstation'; for example see figures 1-2) *comprises*

a trusted hardware module ('trusted path subsystem'; For example see figs. 2-4; col. 4, lines 33-39) *resistant to unauthorized modification* (For example see col. 2, lines 27-38);

a plurality of further hardware modules ('workstation processing unit, display with video manager, keyboard with keyboard manager'; For example see figs. 1-4);

a first communication path ('separate data path' or 'auxiliary data path'; For example see figs. 2-4; col. 4, lines 33-39), *by which a first one* ('workstation processing unit') *of the further hardware modules can communicate directly with the trusted hardware module but cannot communicate directly with any other of the further hardware modules* (For example see figs. 2-4; col. 4, lines 33-50; wherein the workstation processing unit, display, and keyboard, each directly connects to the trusted path subsystem, but not with any other). **Boebert** does disclose the processing unit, display, and keyboard of the workstation ("*plurality of further hardware modules*"; for example see fig. 2) communicate with each other in different modes such as normal and trusted path mode as disclosed in col. 5, lines 20-32; but fails to explicitly disclose, "*a* *shared communication infrastructure*" by which the hardware modules can communicate with each other. However, in order to various system components of the workstation, such as processing unit, display, keyboard, etc., communicate with each other, a system bus has to be provided for communicating and transferring information between elements within the computer or workstation; and such implementation is known in the art.

For example, **Beckman** discloses, a system and method for providing a security framework with security services (for example see col. 5, lines 8-10); wherein, in figure 1, the system bus 23, e.g. "*shared communication infrastructure*", connects the monitor, keyboard and other system components together to the processing unit for communicating and transferring information between elements within the computer or workstation, e.g. "*by which the hardware modules can communicate with each other*", as specified in figure 1; col. 5, line 52 through col. 6, line 7).

Thus it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to include a system bus, e.g. "*shared communication infrastructure*", within the computer or workstation as taught by **Beckman** into the **Boebert**'s workstation, for the purpose of communicating and transferring information between elements within the computer or workstation. The motivation being that distributing tasks in the computer environments as disclosed in **Beckman**: col. 5, lines 44-50.

- Regarding claims 2 and 22, in addition to features in base claims 1 and 21 (see rationales pertaining the rejection of base claims 1 and 21 discussed above), **Boebert** further discloses *wherein the trusted hardware module* ('trusted path subsystem') *and the* *first further hardware module* ('workstation processing unit 40') *each include a respective computing engine* ('processor 31', 'processing unit 40'; For example see Figs 3-4; wherein it is inherent that the workstation processing unit has its own processor for processing the application for the workstation unit) *which partakes in the direct communication via the first communication path* (for example see figure 2; where the workstation processing unit connects to the trusted path subsystem through the separate data path or auxiliary data path, e.g. "*first communication path*").

- In regard to claims 3 and 23, in addition to features in base claims 1 and 21 (see rationales pertaining the rejection of base claims 1 and 21 discussed above), **Boebert** further discloses *wherein the first further hardware module is operable to supply to the trusted hardware module the request for operation on data* ("trusted path mode"; For example see col. 5, lines 17-32; wherein the workstation invokes trusted path mode through different number of ways as disclosed in col. 5, line 66 through col. 6, line 10; e.g. '*request for operation on data*') *and in response to such a request, the trusted hardware module is operable to generate a response* ('feedback mechanism'; for example see col. 6, lines 8-10) *and to supply the response to the first further hardware module via the first communication path* ('separate data path or auxiliary data path 42'; for example see figs. 2-4) *and not via the shared communication infrastructure* (For example see figs. 2-4; col. 5, lines 27-32; wherein each individual element connects to the trusted path subsystem by its own separated path as specified in figure 2). **Boebert** fails to explicitly disclose, "*the shared communication infrastructure*" by which the hardware modules can communicate with each other. However, in order to various system components of the workstation, such as processing unit, display, keyboard, etc., communicate with each other, a system bus has to be provided for communicating and transferring information between elements within the computer or workstation; and such implementation is known in the art.

For example, **Beckman** discloses, a system and method for providing a security framework with security services (for example see col. 5, lines 8-10); wherein, in figure 1, the system bus 23, e.g. "*shared communication infrastructure*", connects the monitor, keyboard and other system components together to the processing unit for communicating and transferring information between elements within the computer or workstation as specified in figure 1; col. 5, line 52 through col. 6, line 7).

Thus it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to include a system bus, e.g. "*shared communication infrastructure*", within the computer or workstation as taught by **Beckman** into the **Boebert**'s workstation, for the purpose of communicating and transferring information between elements within the computer or workstation. The motivation being that distributing tasks in the computer environments as disclosed in **Beckman**: col. 5, lines 44-50.

- In regard to claims 4, 15 and 24, **Boebert** further discloses, *means for storing policy information* ('encryption algorithm in cryptographic entity' in figure 2; col. 5, lines 52-65) *regarding such operations which can or cannot be permitted* ('authentication'), *and is operable to generate the response with reference to the policy information* (for example see col. 6, lines 5-10, 29-34. Though, **Boebert** does not explicitly disclose about "*policy information*"; however, in order to recognizing classified information of varying sensitivity and different levels of users access, the multi-level secure 'MLS' computer (see Figs. 1-2) has to store information about different levels to access to the secure subsystem, e.g. "*policy information*", to provide the access right to users).

- Regarding claims 5 and 25, **Boebert** further discloses, *wherein the trusted hardware module is operable to generate an encryption and/or decryption key* ('pair-wise key' or 'public key') *and supply that key to the first further hardware module via the first communication path* ('separate data path or auxiliary data path 42'; where the workstation processing unit connects to the trusted path subsystem through the separate data path or auxiliary data path in figures 2-4, e.g. "*first communication path*") *and not via the shared communication infrastructure* (where the workstation processing unit connects to the trusted path subsystem through the separate data path or auxiliary data path 42 in figures 2-4). **Boebert** fails to explicitly disclose, "*the shared communication infrastructure*" by which the hardware modules can communicate with each other. However, in order to various system components of the workstation, such as processing unit, display, keyboard, etc., communicate with each other, a system bus has to be provided for communicating and transferring information between elements within the computer or workstation; and such implementation is known in the art.

For example, **Beckman** discloses, a system and method for providing a security framework with security services (for example see col. 5, lines 8-10); wherein, in figure 1, the system bus 23, e.g. "*shared communication infrastructure*", connects the monitor, keyboard and other system components together to the processing unit for communicating and transferring information between elements within the computer or workstation, e.g. "*by which the hardware modules can communicate with each other*", as specified in figure 1; col. 5, line 52 through col. 6, line 7).

Thus it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to include a system bus, e.g. "*shared communication infrastructure*", within the computer or workstation as taught by **Beckman** into the **Boebert**'s workstation, for the purpose of communicating and transferring information between elements within the computer or workstation. The motivation being that distributing tasks in the computer environments as disclosed in **Beckman**: col. 5, lines 44-50.

- Regarding claims 7-8, 20, 27-28 and 30, **Boebert** further discloses, *wherein the trusted hardware module is operable to generate a challenge and to supply the challenge to the first further hardware module via the first communication path or via the shared communication infrastructure using encryption set up using the first communication path* (For example see col. 6, lines 26-39; wherein, in order to access the system, the user from the workstation has to provide the personal identification number 'PIN', password, biometric or token device to authenticate himself to the secure subsystem, where the "*challenge*" from the subsystem such as the login window is obvious and well known in the art); *and wherein, in response to the challenge, the first further hardware module is operable to generate a response and to supply the response the trusted hardware module via the first communication path the shared communication infrastructure using encryption set up using the first communication path* (For example see col. 6, lines 26-39;

wherein the user provides the personal identification number 'PIN', password, biometric or token device to authenticate himself to the subsystem in order to access the secure system). Though, **Boebert** does not explicitly disclose about "*integrity metric*"; however, it is obvious that information such as personal identification number 'PIN', password, biometric or token device are used to authenticate the user to the secure subsystem and are the "*integrity metric*", which create and store by the trusted system, in order to provide classified information of varying sensitivity and different levels of users access right for different user.

Thus it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to combine the implementation "*integrity metric*" into the **Boebert**'s trusted subsystem, with the motivation being to provide classified information of varying sensitivity and different levels of users access right for different user.

- In regard to claims 12 and 29, **Boebert** further discloses, *wherein the first further hardware module is a network interface module* (for example see figures 2-4; wherein the working processing unit connects to the network 50, e.g. "*network interface module*").

- In regard to claims 13 and 18, **Boebert** further discloses, the second communication and third communication path, distinct from the shared communication infrastructure and the first communication path, by which the second one, e.g. 'display 10', and the third one, e.g. 'keyboard 20', of the further hardware modules communicate directly with the trusted past subsystem with separated connection in trusted path mode and cannot communicate directly with any other of the further hardware modules such as the workstation processing unit 40 as in trusted path mode ("*second and third communication paths*"; for example see figs. 2-4).

- Regarding claims 14 and 16, **Boebert** further discloses, *wherein the first further hardware module is operable to supply to the trusted hardware module a request for a transfer of data between the first and second further hardware modules* ('trusted path mode'; for example see col. 5, lines 17-32; wherein the workstation invokes trusted path mode through different number of ways as disclosed in col. 5, line 66 through col. 6, line 10; e.g. '*request for a transfer of data*') *and in response to such a request, the trusted hardware module is operable to generate a response* ('feedback mechanism'; For example see col. 6, lines 8-10) *and to supply the response to the first or second further hardware module via the first or second communication path* ('separate data path or auxiliary data path 42'; for example see figs. 2-4), *not via the shared communication infrastructure* (for example see figs. 2-4; col. 5, lines 27-32; wherein each individual element connects to the trusted path subsystem by its own separated path as specified in figure 2); *and wherein the trusted hardware module is operable to relay the data to the second or first further hardware module via the second or first communication path* as claimed in the claim invention 16 (For example see col. 6, lines 34-39). **Boebert** fails to explicitly disclose, "*the shared communication infrastructure*" by which the hardware modules can communicate with each other. However, in order to various system components of the workstation, such as processing unit, display, keyboard, etc., communicate with each other, a system bus has to be provided for communicating and transferring information between elements within the computer or workstation; and such implementation is known in the art.

For example, **Beckman** discloses, a system and method for providing a security framework with security services (for example see col. 5, lines 8-10); wherein, in figure 1, the system bus 23, e.g. "*shared communication infrastructure*", connects the monitor, keyboard and other system components together to the processing unit for communicating and transferring information between elements within the computer or workstation as specified in figure 1; col. 5, line 52 through col. 6, line 7).

Thus it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to include a system bus, e.g. "*shared communication infrastructure*", within the computer or workstation as taught by **Beckman** into the **Boebert**'s workstation, for the purpose of communicating and transferring information between elements within the computer or workstation. The motivation being that distributing tasks in the computer environments as disclosed in **Beckman**: col. 5, lines 44-50.

- In regard to claims 17 and 19, **Boebert** further discloses about the display 10 (for example see figs. 1-4) and video RAM in the video manager ("*non-volatile data storage module*"; For example see Fig. 5; col. 8, lines 51-63).

Response to Amendment/Arguments

6. Applicant's arguments filed on June 16th, 2006 with respect to claims 1-30 have been considered but are moot in view of the new ground(s) of rejection.

Allowable Subject Matter

7. Claims 6, 9-11 and 26 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

Many references in the art disclose the system and method for secure communication in trusted subsystem for workstation. Most of those references comprise various system components of the workstation, such as workstation processing unit, display, keyboard, and trusted path subsystem that found in Boebert et al. et al [U.S. 5,822,435]. But no prior art reference utilizes the separate zone for private and non-private data in the hardware module through different paths.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tri H. Phan, whose telephone number is (571) 272-3074. The examiner can normally be reached on M-F (8:00-4:30).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chi H. Pham can be reached on (571) 272-3179.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, D.C. 20231

or faxed to:

(571) 273-8300

Hand-delivered responses should be brought to Randolph Building, 401 Dulany Street, Alexandria, VA 22314.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Technology Center 2600 Customer Service Office, whose telephone number is (571) 272-2600.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Tri H. Phan
August 24, 2006

CHI PHAM
SUPERVISORY PATENT EXAMINER 8/25/06